# NetBrain for CMMC Compliance

## THE CMMC CHALLENGE

The federal government released the first version of the Cybersecurity Maturity Model Certification (CMMC) on January 30, 2020. CMMC is a security framework designed to reduce exfiltration of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) from contractors doing business with the Department of Defense (DoD).

CMMC defines five security maturity levels that draw heavily on existing frameworks such as FAR, DFAR, FIPS, NIST 800-171 and others. Each DoD contract will be aligned with a specific CMMC level based on the type and sensitivity of the data. Prior to bidding a contract, bidders are required to have third-party certification that verifies their business environment meets the associated CMMC security level. The government defines each maturity level with the following criteria:

- Level 1: Safeguard Federal Contract Information (FCI)
- Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3: Protect Controlled Unclassified Information (CUI)
- Levels 4-5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

CMMC creates significant challenges for the roughly 300,000 companies doing business with the DoD. And a large portion of the security controls making up each maturity level involve analyzing network devices for configuration vulnerabilities and creating documentation such as network diagrams and asset inventory lists. Because of the complexity of today's networks, manually gathering and assembling this information can take many months, even for small networks.

For ongoing CMMC compliance, continuous verification is required, with recertification mandated every three years for CMMC levels 1 and 2, every two years for level 3, and annually for levels 4 and 5.

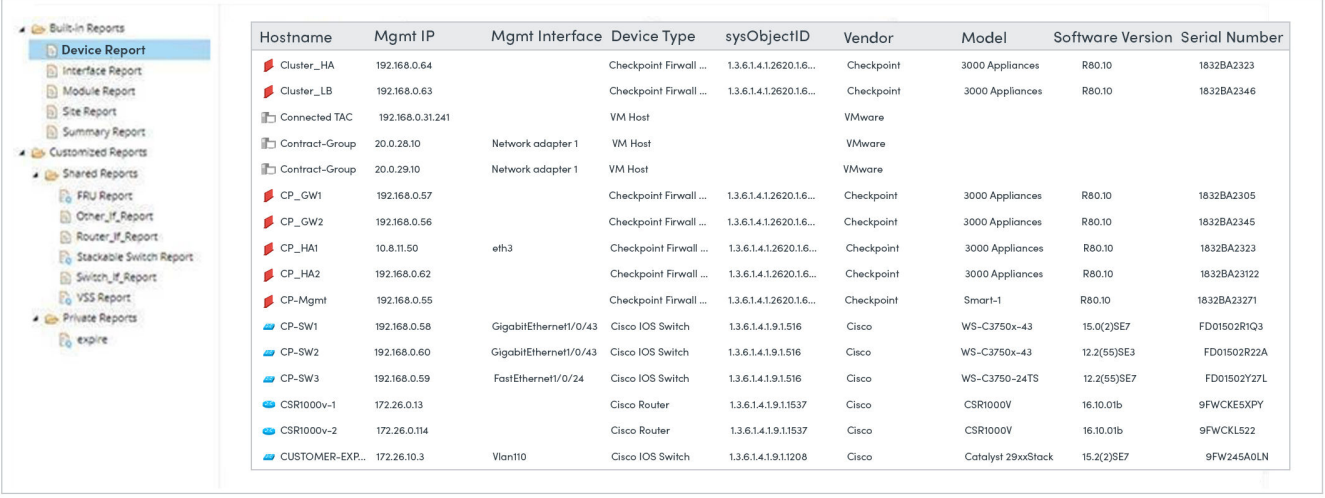
## HOW NETBRAIN AUTOMATION HELPS

NetBrain is a robust network automation platform that delivers dynamic mapping, compliance verification, asset inventory, IP and MAC address reporting, configuration, change management, and network troubleshooting. NetBrain can be leveraged for the networking requirements of both pre-certification assurance to eliminate compliance overhead and as an ongoing safeguard to mitigate post-certification liabilities.

### Quickly Develop Asset Inventories

Using a combination of SNMP, command-line interface (CLI), and REST API, NetBrain rapidly discovers up to 3,000 devices per hour in multi-vendor environments. With direct integrations for more than 150 of the most common networking vendors, and extensions to many more via API, the NetBrain discovery process gathers platform and configuration data from all devices on traditional, SDN, SD-WAN, and public cloud networks to determine their interconnections for dynamic network mapping.

The resulting data delivers an extensive asset inventory that details device vendor, platform type, firmware levels, OS types, modules, serial numbers, and much more. The inventory reports can also be configured to pull data from other inventory systems or data tables to include elements such as asset tags, end-of- life dates, and configuration verifications.

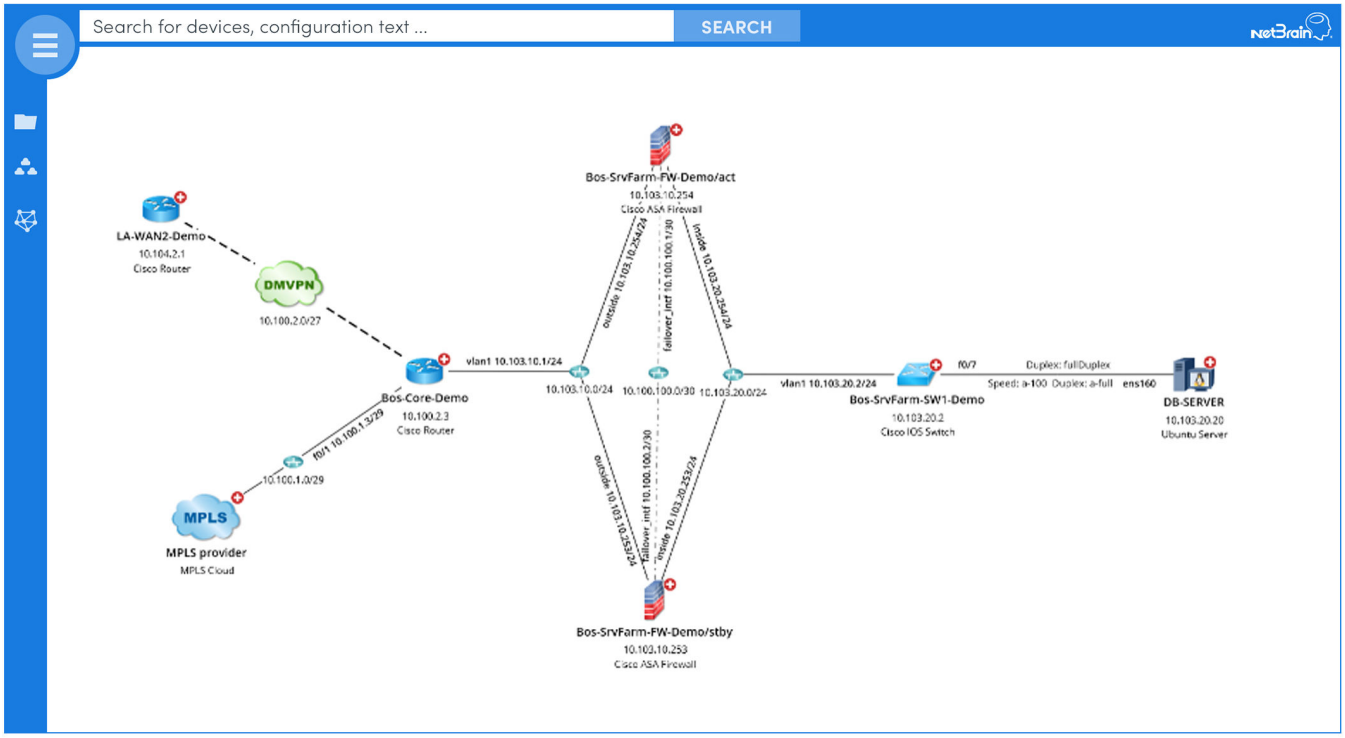



| Hostname | Mgmt IP | Mgmt Interface | Device Type | sysObjectID | Vendor | Model | Software Version | Serial Number |
|---|---|---|---|---|---|---|---|---|
| Cluster_HA | 192.168.0.64 | | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | 3000 Appliances | R80.10 | 1832BA2323 |
| Cluster_LB | 192.168.0.63 | | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | 3000 Appliances | R80.10 | 1832BA2346 |
| Connected TAC | 192.168.0.31.241 | | VM Host | | VMware | | | |
| Contract-Group | 20.0.28.10 | Network adapter 1 | VM Host | | VMware | | | |
| Contract-Group | 20.0.29.10 | Network adapter 1 | VM Host | | VMware | | | |
| CP_GW1 | 192.168.0.57 | | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | 3000 Appliances | R80.10 | 1832BA2305 |
| CP_GW2 | 192.168.0.56 | | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | 3000 Appliances | R80.10 | 1832BA2345 |
| CP_HA1 | 10.8.11.50 | eth3 | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | 3000 Appliances | R80.10 | 1832BA2323 |
| CP_HA2 | 192.168.0.62 | | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | 3000 Appliances | R80.10 | 1832BA23122 |
| CP-Mgmt | 192.168.0.55 | | Checkpoint Firwall ... | 1.3.6.1.4.1.2620.1.6... | Checkpoint | Smart-1 | R80.10 | 1832BA23271 |
| CP-SW1 | 192.168.0.58 | GigabitEthernet1/0/43 | Cisco IOS Switch | 1.3.6.1.4.1.9.1.516 | Cisco | WS-C3750x-43 | 15.0(2)SE7 | FD01502R1Q3 |
| CP-SW2 | 192.168.0.60 | GigabitEthernet1/0/43 | Cisco IOS Switch | 1.3.6.1.4.1.9.1.516 | Cisco | WS-C3750x-43 | 12.2(55)SE3 | FD01502R22A |
| CP-SW3 | 192.168.0.59 | FastEthernet1/0/24 | Cisco IOS Switch | 1.3.6.1.4.1.9.1.516 | Cisco | WS-C3750-24TS | 12.2(55)SE7 | FD01502Y27L |
| CSR1000v-1 | 172.26.0.13 | | Cisco Router | 1.3.6.1.4.1.9.1.1537 | Cisco | CSR1000V | 16.10.01b | 9FWCKE5XPY |
| CSR1000v-2 | 172.26.0.114 | | Cisco Router | 1.3.6.1.4.1.9.1.1537 | Cisco | CSR1000V | 16.10.01b | 9FWCKL522 |
| CUSTOMER-EXP... | 172.26.10.3 | Vlan110 | Cisco IOS Switch | 1.3.6.1.4.1.9.1.1208 | Cisco | Catalyst 29xxStack | 15.2(2)SE7 | 9FW245A0LN |

NetBrain automatically generates a complete inventory of every device on a network in hours.

## Network Mapping

While useful, a network addressing database is difficult to verify without accompanying network diagrams. NetBrain dynamically maps the interconnections between devices and provides views into the physical underlay and virtual, tunneled overlay connections with accompanying IPv4 and IPv6 address assignments. Focused attention can then be applied to specific network segments – like public security boundaries – to ensure compliant IP subnetting is in use. With daily, automated map updates, auditors can be confident that maps reflect the current state of the network.

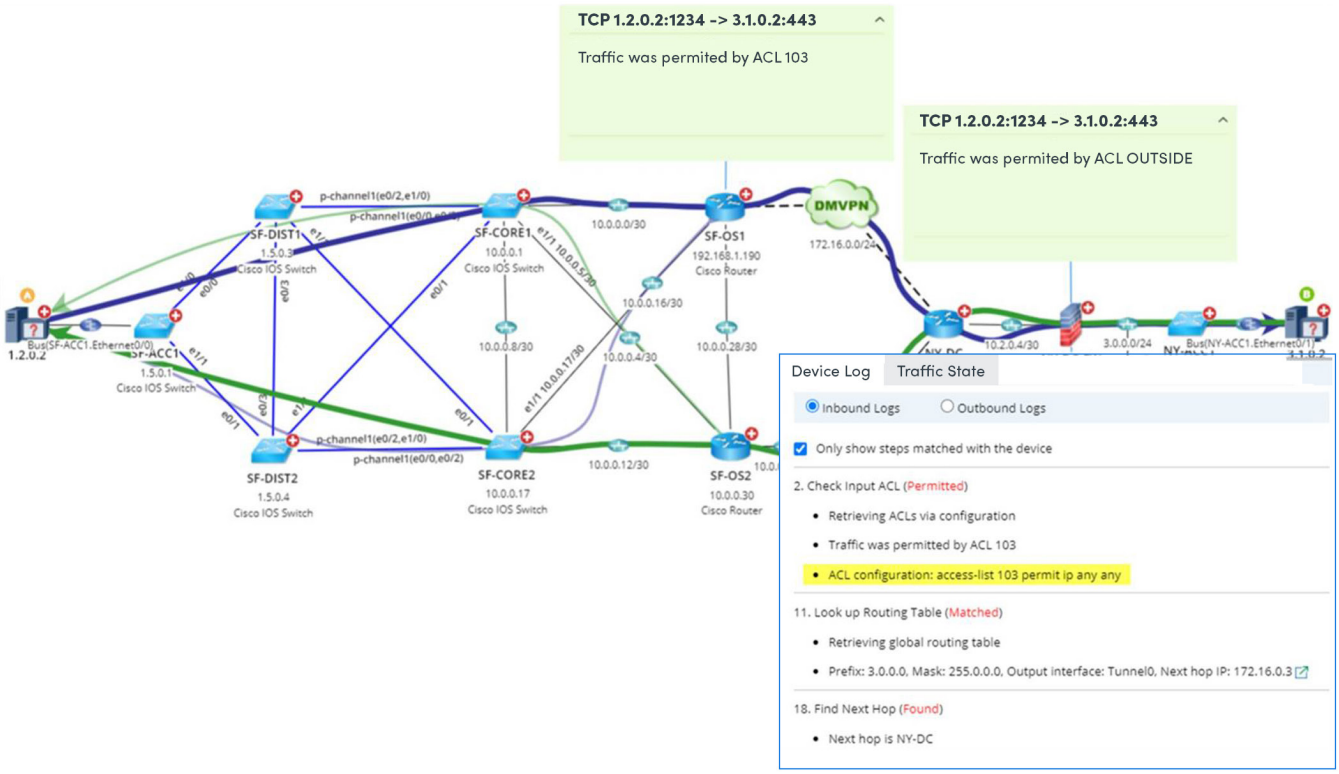



Dynamic Mapping delivers up-to-date maps that provide rich detail about the current state of the network.

## Proving Data Boundaries

NetBrain A-B Path Mapping verifies how traffic between hosts using specified TCP or UDP ports transits the network. Starting at the source device gateway interface, NetBrain builds the layer 2 and 3 destination paths by querying each device's switching tables, route tables, policy-based routing configurations, NAT, IPsec, and MPLS VPN configurations to determine

the exact path taken. NetBrain will also identify if the traffic profile is permitted or denied by any router, switch, or firewall access lists along the way. This is all done without requiring live traffic, which allows verifications to take place at any time without needing access to the source and destination devices.

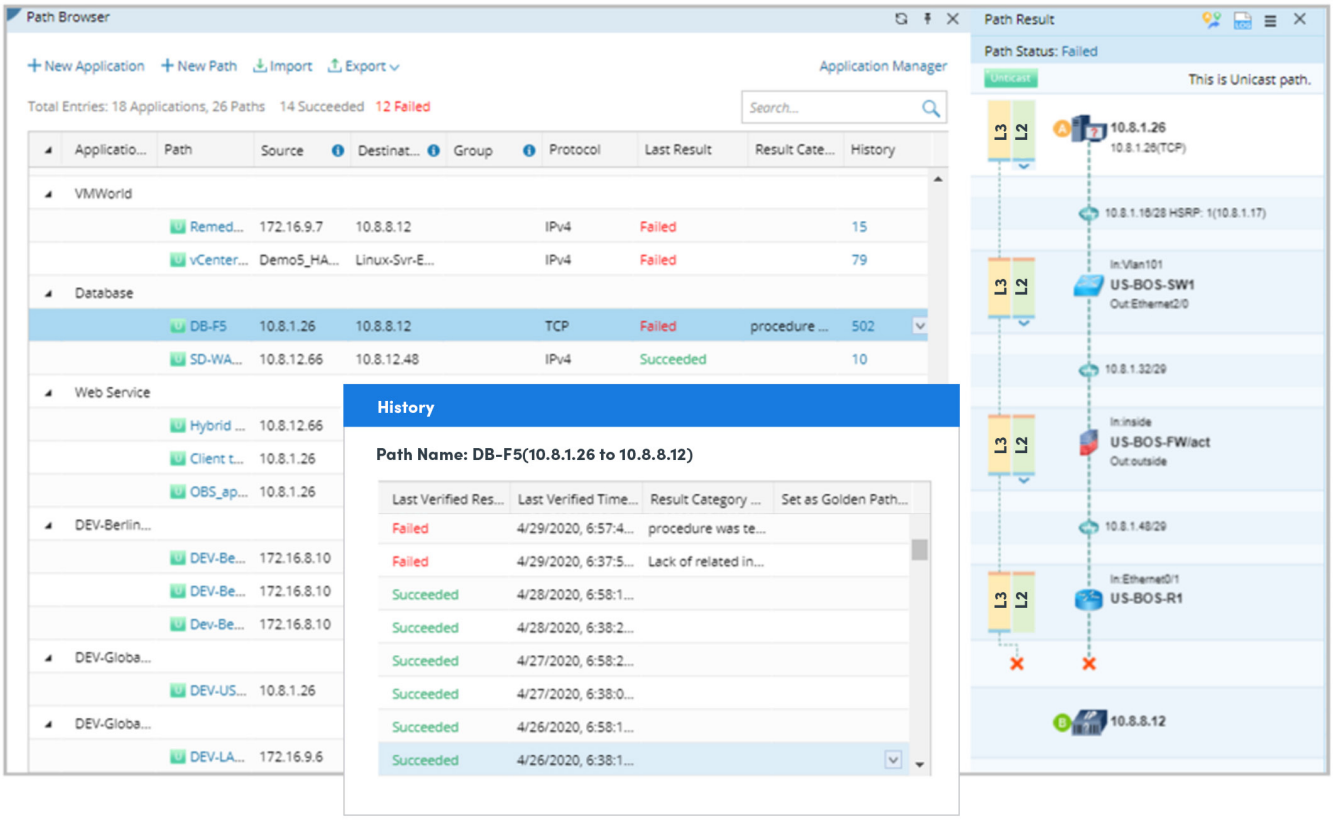



NetBrain delivers information on every device across critical paths to prove out data boundaries.

## Continuous Analysis of Data Boundaries

The NetBrain Application Assurance Module (AAM) expands on A-B Path Mapping to enable continual path verification. By testing paths at configurable intervals, administrators are alerted when paths change between specified hosts indicating possible problems within the network, as well as identifying paths that might not flow through the proper security equipment. Certain paths can be set up that are intended to fail, such as paths from subnets that should be prevented from accessing certain resources. NetBrain will alert administrators

when these paths succeed, indicating a misconfiguration in security access lists that are now incorrectly allowing traffic to specified resources.




The Application Assurance Module alerts administrators to possible security violations in critical paths.

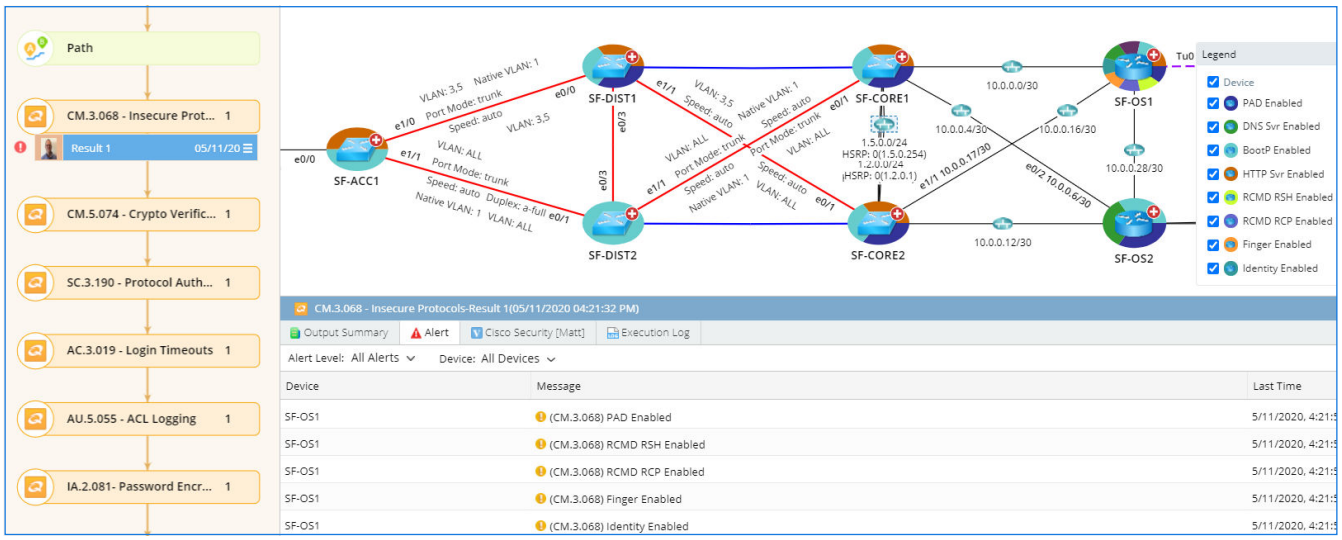
## Improved Change Management

Customized reports are used to determine whether mandated configurations are in place or if device vulnerabilities are present (e.g. the use of unsecured protocols). Daily benchmarking activities will discover new devices added to the network to continuously verify compliance. Email alerts notify system administrators as new devices are discovered or when device configurations experience drift.

As vulnerabilities are uncovered, NetBrain's change management features provide a methodical framework for establishing and documenting the remediation changes, specifying the change window, and requesting approval. Role-based access control (RBAC) provides separate authorizations for approving and executing changes. Only approved changes (and their rollback configurations) can be applied during the specified change window. If desired, Ansible playbooks can be utilized in the NetBrain change management framework.

## NetBrain CMMC Runbooks

NetBrain has worked with several customers to accelerate the adoption of best practices for automating CMMC compliance. This includes the creation of a series of NetBrain Executable Runbooks that are labeled with the CMMC Practice Requirements. Available to all customers, the CMMC Runbooks automate important steps in the CMMC compliance process, allowing any network engineer to deliver the documentation and network maps for crucial CMMC Practice Requirements.




NetBrain's CMMC Runbooks gather and document important network information for CMMC compliance.

## Support Across 14 of 17 Domains

Each CMMC security maturity level maps to components within 17 domains. The diagram below highlights the domains where NetBrain automation provides significant capabilities towards meeting the CMMC requirements.

| | | | | |
|---|---|---|---|---|
| Access Control (AC) | Access Management (AM) | Audit and Accountability (AU) | Awareness and Training (AT) | Configuration Management (CM) |
| Identification and Authentication (IA) | Incident Response (IR) | Maintenance (MA) | Media Protection (MP) | Personnel Security (PS) |
| Physical Protection (PE) | Recovery (RE) | Risk Management (RM) | Security Assessment (CA) | Situational Awareness (SA) |
| | System and Communications Protection (SC) | System and Information Integration (SI) | | |

## IN SUMMARY

Meeting the network documentation, vulnerability analysis, and remediation requirements specified in CMMC can be a daunting manual task. NetBrain automation reduces the time and manpower to comply with the network-based requirements of CMMC by as much as 90%, resulting in significant cost savings both in the initial audit preparation time and in post-audit activities. Faster audits allow contractors to bid on jobs sooner than their competitors. Daily automated benchmarking and discovery ensures that network compliance is maintained for future recertifications.

## Seeing is Believing

See an engineer-to-engineer demo of NetBrain's CMMC capabilities by requesting a demo.

**About NetBrain**

Founded in 2004, NetBrain is the market leader for network automation. The NetBrain platform automates the resolution of every network incident, helping NetOps teams resolve 100s or 1,000s of tickets daily. Today, more than 2,400 of the world's largest enterprises and managed services providers use NetBrain to automate network troubleshooting, accelerate change management and documentation, and strengthen network security — all while integrating with a rich ecosystem of network management tools. NetBrain has significant penetration in the federal space, including DoD, Intel, FSI, and civilian agencies.

Available contracts via teaming: GSA, SEWP, CHESS

DUN & Bradstreet: 82-740-6724

Cage Code: 5FHR3

NAICS Code(s): 511210 Software Publishers; 541511 Customer Computer Programming Services

Compliance: FIPS 140-2